

ILLEGAL ACCESS PREVENTION METHOD AND SYSTEM

Patent number: JP10271154

Publication date: 1998-10-09

Inventor: MATSUOKA YOSHIE

Applicant: NEC ENG LTD

Classification:

- international: H04L12/46; H04L12/28; H04L9/32; H04L9/36;
H04L12/56

- european:

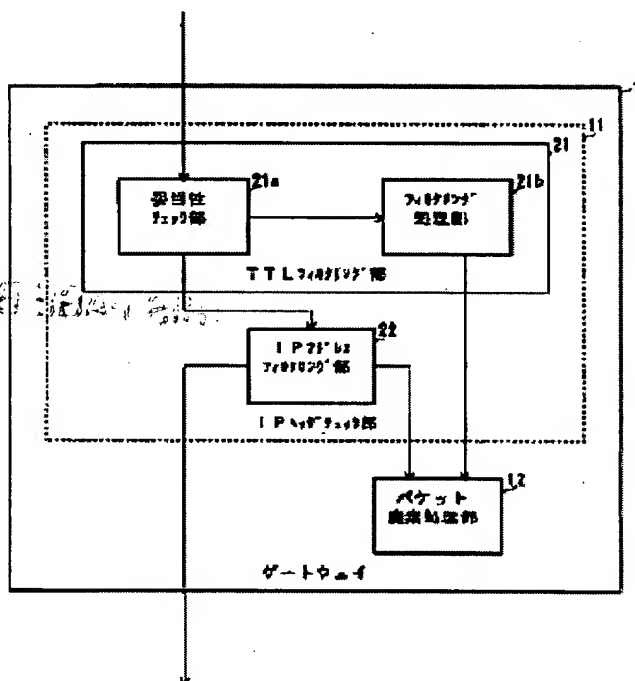
Application number: JP19970067929 19970321

Priority number(s):

Abstract of JP10271154

PROBLEM TO BE SOLVED: To exclude an illegal packet by means of filtering utilizing an existing area of a packet without adding an area to a packet data form.

SOLUTION: An IP header check section 11 of a gateway 1 passes only a legal communication packet based on TT (Time To Live: in-network duration time) information and IP address information included in an IP header. A TTL filtering section 21 of the IP header check section 11 passes only a communication packet having valid TTL information in the IP header. A validity check section 21a checks the validity under the condition that the value of the TTL at packet passing is within a range from a predetermined initial value in a group in advance to a (initial value-maximum passing gateway number). The filtering processing section 21b gives a communication packet whose TTL information does not satisfy a prescribed condition to a packet abort processing section 12.



THIS PAGE BLANK (USPTO)

(51) Int.Cl.⁶

識別記号

F I

H 0 4 L 12/46
12/28
9/32
9/36
12/56

H 0 4 L 11/00 3 1 0 C
9/00 6 7 1
6 8 5
11/20 1 0 2 Z

審査請求 未請求 請求項の数10 O L (全 10 頁)

(21) 出願番号

特願平9-67929

(22) 出願日

平成9年(1997)3月21日

(71) 出願人 000232047

日本電気エンジニアリング株式会社
東京都港区芝浦三丁目18番21号

(72) 発明者 松岡 芳恵

東京都港区芝浦三丁目18番21号 日本電気
エンジニアリング株式会社内

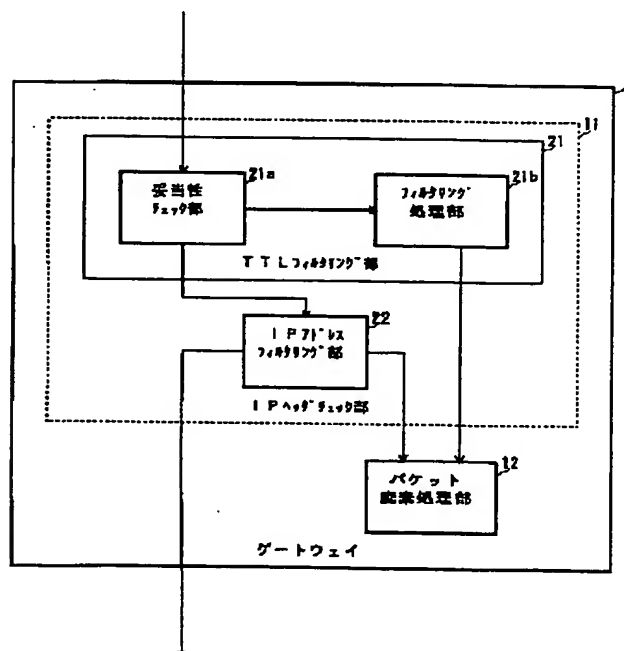
(74) 代理人 弁理士 鈴木 正剛

(54) 【発明の名称】 不正アクセス防止方法およびシステム

(57) 【要約】

【課題】 パケットのデータ形式にエリアの追加を行うことなく、パケットの既存エリアを利用した不正パケットのフィルタリングによる排除を可能とする。

【解決手段】 ゲートウェイ1のIPヘッダチェック部11は、IPヘッダに含まれるTTL (Time To Live: ネットワーク内生存時間) 情報およびIPアドレス情報に基づいて、不正でない通信パケットのみを通過させる。IPヘッダチェック部11のTTLフィルタリング部21は、IPヘッダ中に妥当性のあるTTL情報を有する通信パケットのみを通過させる。妥当性チェック部21aは、パケット通過時のTTLの値が、予めグループ内で取り決めた初期値から(初期値-最大通過ゲートウェイ数)までの範囲内であることを条件として妥当性をチェックする。フィルタリング処理部21bはTTL情報が所定の条件を満足していない通信パケットをパケット廃棄処理部12に与える。



【特許請求の範囲】

【請求項1】 複数の支線ネットワークが結合装置により結合されたネットワーク内に1以上の論理グループが構成されている通信ネットワークにおいて、該論理グループにおける不正アクセスを防止するにあたり、送信時の通信パケットに含まれるネットワーク内持続時間情報の初期値を、予め通信ネットワーク内に設定した論理グループ内における機密情報として、所定値に定めておき、

前記結合装置が、前記通信パケットの通過時に前記ネットワーク内持続時間情報の妥当性をチェックすることにより、前記論理グループの内外間での通過パケットのフィルタリングを行うようにした、ことを特徴とする不正アクセス防止方法。

【請求項2】 前記ネットワーク内持続時間情報は、前記結合装置の通過毎に減算される情報を含み、且つ前記機密情報としてのネットワーク内持続時間情報の初期値は、ネットワーク構成に基づいて予想される前記結合装置の最大通過数を超える値に設定するとともに、前記ネットワーク内持続時間情報の値が、前記初期値乃至前記初期値ー前記最大通過数の範囲外である場合に前記結合装置が当該パケットを不正パケットと判断することを特徴とする請求項1に記載の不正アクセス防止方法。

【請求項3】 IP（インターネットプロトコル）アドレスに基づくフィルタリングをさらに併用することを特徴とする請求項1または2に記載の不正アクセス防止方法。

【請求項4】 MAC（メディアアクセス制御）アドレスに基づくフィルタリングをさらに併用することを特徴とする請求項1乃至3のうちのいずれか1項に記載の不正アクセス防止方法。

【請求項5】 前記不正パケットは、前記結合装置が廃棄することを特徴とする請求項1乃至4のうちのいずれか1項に記載の不正アクセス防止方法。

【請求項6】 複数の支線ネットワークが結合されたネットワーク内に1以上の論理グループが構成されている通信ネットワークシステムにおいて、前記支線ネットワークに結合され、通信パケットの送信時に、該通信パケットに含まれるネットワーク内持続時間情報の初期値を、予め通信ネットワーク内に設定した論理グループ内における機密情報として、所定値に設定するネットワーク内持続時間情報設定手段を有する端末装置と、前記通信パケットの通過時に前記ネットワーク内持続時間情報の妥当性をチェックする妥当性チェック手段、および該妥当性チェック手段のチェック結果に基づいて、前記論理グループの内外間での通過パケットをフィルタリングするフィルタリング処理手段を有し、前記複数の支線ネットワークを結合するとともに、該論理グループにおける不正アクセスを防止するネットワーク結合手段

と、を具備することを特徴とする不正アクセス防止システム。

【請求項7】 前記ネットワーク内持続時間情報は、前記ネットワーク結合手段の通過毎に減算される情報を含み、且つネットワーク内持続時間設定手段は、前記機密情報としてのネットワーク内持続時間情報の初期値を、ネットワーク構成に基づいて予想される前記ネットワーク結合手段の最大通過数を超える値に設定する手段を含むとともに、前記妥当性チェック手段は、前記ネットワーク内持続時間情報の値が、前記初期値乃至前記初期値ー前記最大通過数の範囲外である場合に当該パケットを不正パケットと判断する手段を含むことを特徴とする請求項6に記載の不正アクセス防止システム。

【請求項8】 前記ネットワーク結合手段は、IP（インターネットプロトコル）アドレスに基づくフィルタリングを行うIPアドレスフィルタリング手段をさらに含むことを特徴とする請求項6または7に記載の不正アクセス防止システム。

【請求項9】 前記ネットワーク結合手段は、MAC（メディアアクセス制御）アドレスに基づくフィルタリングを行うMACアドレスフィルタリング手段をさらに含むことを特徴とする請求項6乃至8のうちのいずれか1項に記載の不正アクセス防止システム。

【請求項10】 前記ネットワーク結合手段は、フィルタリングによって通過が阻止された不正パケットを廃棄するパケット廃棄手段を含むことを特徴とする請求項6乃至9のうちのいずれか1項に記載の不正アクセス防止システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、通信ネットワークシステムを構築するルータおよびゲートウェイ等における不正アクセスの防止に係り、特に、通信プロトコルとしてTCP/IP（Transmission Control Protocol / Internet Protocol：転送制御プロトコル／インターネットプロトコル）を使用している通信ネットワークシステムに好適な不正アクセス防止システムに関する。

【0002】

【従来の技術】 通信ネットワークシステム、例えばLAN（Local Area Network：ローカルエリアネットワーク）システムは、ルータおよびゲートウェイの少なくともいずれかを介して複数の支線LANが接続されて構築されている。このような通信ネットワークシステムにおいて、通信プロトコルとしてTCP/IPを使用していることも多い。

【0003】 ところで、物理的に接続されているネットワーク上で、必要に応じて論理的にグループ分けを行っている場合がある。このような場合、論理的なグループ内での通信が主体となつて、他のグループとの間の通信を、必要としなかったり、排除したりしたいことがあ

る。

【0004】このような場合には、支線LANを接続するルータおよびゲートウェイ等において、パケットのMAC (Media Access Control: メディアアクセス制御) アドレスまたはIP (Internet Protocol: インターネットプロトコル) アドレスを識別し、他のグループのパケットを通過させないようにして、同報パケット、異常パケット、あるいは不正に他のグループの端末にアクセスしようとするパケット等の不正アクセスパケットの流入および流出を防止することが行われている。

【0005】このように、パケットのMACアドレスまたはIPアドレスを識別して他のグループのパケットは通過させないようにする機能は、MACアドレスによりフィルタリングを行うMACアドレスフィルタリング機能またはIPアドレスによりフィルタリングを行うIPアドレスフィルタリング機能と称される。

【0006】すなわち、MACアドレスまたはIPアドレスによるフィルタリングは、次のようにして行われる。予め通過を許容するMACアドレスまたはIPアドレスを、ルータあるいはゲートウェイに登録しておく。ルータあるいはゲートウェイは、受信したパケットのMACアドレスまたはIPアドレスと登録されているMACアドレスまたはIPアドレスとを照合して、正しいMACアドレスまたはIPアドレスのパケットのみを通過させる。このようにして、不正アクセスパケットの通過がルータあるいはゲートウェイにより阻止される。

【0007】MACアドレスは、多くの場合端末装置（以下、単に「端末」と称する）に物理的に設定されており、安易に変更することができないことが多い。ところが、MAC層アドレスには、全ネットワークに同報パケットを通過させるための同報アドレスが存在するため、同報パケットとの混同が生じる。これを防止するために、MAC層よりも上位層であるネットワーク層のIPアドレスでフィルタリングするIPアドレスフィルタリングが用いられる。

【0008】しかしながら、IPアドレスは、TCP/IPプロトコルに必要なものであり、装置に論理的に設定しているため、比較的容易に変更することが可能である。そのため、グループ外の端末が、当該グループ内の端末のIPアドレスを不正に設定してグループ内のLANシステムに入り込もうとした場合には、IPアドレスのフィルタリングでは、不正アクセスパケットを確実に検出することができない。

【0009】これに対して、特開平7-170279号公報には、IPアドレスフィルタリングを用いることなく、不正アクセスパケットを排除する技術が開示されている。

【0010】すなわち、特開平7-170279号公報に示されたシステムは、MACアドレスによるフィルタリングを行う複数の支線LANを収容する従来のブリッ

ジ回路に対して、支線LANのグループ番号を登録する機能、パケット送信時に該グループ番号をパケットに付加する機能、およびパケットに付加されたグループ番号と登録されたグループ番号とをパケット受信時に照合する機能を付加したブリッジ回路を用いる。

【0011】このブリッジ回路に収容したLANそれぞれにグループ番号を設定し、同一グループ内のLAN間転送時には基幹バスへ送信するパケットに、該グループ番号を付加する。基幹バスからパケットを受信するときはブリッジ回路が元来行っていたフィルタリング機能であるMACアドレスによるフィルタリングを行う前に、送信時にパケットに付加されたグループ番号によるフィルタリングを行う。

【0012】すなわち、複数の端末が接続される複数の支線LANを複数のブリッジ回路を介して基幹バスに接続するシステムにおいて、複数のブリッジ回路に個々に収容された複数の支線LANを独立した複数のグループにグループ化し、各ブリッジ回路にはそれぞれ収容する支線LANのグループ番号を予め登録しておく。端末から同一グループ内の他の支線LANへ送信するパケットには、ブリッジ回路は、該端末が属する支線LANのグループ番号を付加して基幹バスに送信する。基幹バスを介してパケットを受信したときには、ブリッジ回路は、受信したパケットに付加されているグループ番号を識別し、登録されている番号と照合して、両者が一致したときにのみ、この受信したパケットに対してMACアドレスフィルタリング機能を動作させブリッジ回路が収容している支線LANに送信する。

【0013】このようにすることにより、LANのMAC層における同報パケット、異常パケットまたは不正に他のグループの端末に他のグループの端末と通信しようとするパケット等の不正アクセスパケットを、グループ番号の相違により阻止することができる。

【0014】

【発明が解決しようとする課題】上述したように、特開平7-170279号公報に示されたシステムは、ブリッジ回路に収容した複数のLANにそれぞれグループ番号を設定し、同一グループ内のLAN間転送時には基幹バスへ送信するパケットに、該グループ番号を付加する。基幹バスからパケットを受信するときはブリッジ回路が元来行っていたフィルタリング機能であるMACアドレスによるフィルタリングを行う前に、送信時にパケットに付加されたグループ番号によるフィルタリングを行う。

【0015】この特開平7-170279号公報のシステムによれば、グループ番号の相違をチェックすることにより、LANのMAC層における同報パケット、異常パケットまたは不正に他のグループの端末に他のグループの端末と通信しようとするパケット等の不正アクセスパケットを阻止することができる。

【0016】しかしながら、特開平7-170279号公報に示された、ブリッジ回路にグループ番号を登録し、送信パケットにこのグループ番号を付加して、パケットを受信したときに受信パケットのグループ番号と登録したグループ番号の照合を行うフィルタリングを可能とするためには、パケットのデータ形式にグループ番号エリアを追加する必要がある。

【0017】ところが、LANのパケットには、物理層のヘッダ部およびトランスポート層のヘッダ部等が含まれており、パケットのデータ形式が細かく規定されることが多い。したがって、パケットのデータ形式が規定されているLANシステムにおいては、多くの場合、在来のパケットにグループ番号を格納するためのエリアを追加して確保することができず、特開平7-170279号公報に記載された技術を実施することができない。

【0018】この発明は、上述した事情に鑑みてなされたもので、パケットの既存エリアを利用した不正パケットのフィルタリングを可能とし、パケットのデータ形式にエリアの追加を行うことなく、不正パケットの効果的な排除を可能とする不正アクセス防止方法およびシステムを提供することを目的とする。

【0019】

【課題を解決するための手段】上記目的を達成するため、この発明の第1の観点に係る不正アクセス防止方法は、複数の支線ネットワークが結合装置により結合されたネットワーク内に1以上の論理グループが構成されている通信ネットワークにおいて、該論理グループにおける不正アクセスを防止するにあたり、送信時の通信パケットに含まれるネットワーク内継続時間情報の初期値を、予め通信ネットワーク内に設定した論理グループ内における機密情報として、所定値に定めておき、前記結合装置が、前記通信パケットの通過時に前記ネットワーク内継続時間情報の妥当性をチェックすることにより、前記論理グループの内外間での通過パケットのフィルタリングを行うようにする。

【0020】前記ネットワーク内継続時間情報は、前記結合装置の通過毎に減算される情報を含み、且つ前記機密情報としてのネットワーク内継続時間情報の初期値は、ネットワーク構成に基づいて予想される前記結合装置の最大通過数を超える値に設定するとともに、前記ネットワーク内継続時間情報の値が、前記初期値乃至前記初期値ー前記最大通過数の範囲外である場合に前記結合装置が当該パケットを不正パケットと判断するようにしてもよい。

【0021】前記不正アクセス防止方法は、さらに、IPアドレスに基づくフィルタリングをさらに併用するようにしてもよい。

【0022】前記不正アクセス防止方法は、さらに、MACアドレスに基づくフィルタリングをさらに併用する

ようにしてもよい。

【0023】前記不正アクセス防止方法は、前記不正パケットを、前記結合装置が廃棄するようにしてもよい。

【0024】この発明の第2の観点に係る不正アクセス防止システムは、複数の支線ネットワークが結合されたネットワーク内に1以上の論理グループが構成されている通信ネットワークシステムにおいて、前記支線ネットワークに結合され、通信パケットの送信時に、該通信パケットに含まれるネットワーク内継続時間情報の初期値を、予め通信ネットワーク内に設定した論理グループ内における機密情報として、所定値に設定するネットワーク内継続時間情報設定手段を有する端末装置と、前記通信パケットの通過時に前記ネットワーク内継続時間情報の妥当性をチェックする妥当性チェック手段、および該妥当性チェック手段のチェック結果に基づいて、前記論理グループの内外間での通過パケットをフィルタリングするフィルタリング処理手段を有し、前記複数の支線ネットワークを結合するとともに、該論理グループにおける不正アクセスを防止するネットワーク結合手段と、を具備する。

【0025】前記ネットワーク内継続時間情報は、前記ネットワーク結合手段の通過毎に減算される情報を含み、且つネットワーク内継続時間設定手段は、前記機密情報としてのネットワーク内継続時間情報の初期値を、ネットワーク構成に基づいて予想される前記ネットワーク結合手段の最大通過数を超える値に設定する手段を含むとともに、前記妥当性チェック手段は、前記ネットワーク内継続時間情報の値が、前記初期値乃至前記初期値ー前記最大通過数の範囲外である場合に当該パケットを不正パケットと判断する手段を含んでいてもよい。

【0026】前記ネットワーク結合手段は、IPアドレスに基づくフィルタリングを行うIPアドレスフィルタリング手段をさらに含んでいてもよい。

【0027】前記ネットワーク結合手段は、MACアドレスに基づくフィルタリングを行うMACアドレスフィルタリング手段をさらに含んでいてもよい。

【0028】前記ネットワーク結合手段は、フィルタリングによって通過が阻止された不正パケットを廃棄するパケット廃棄手段を含んでいてもよい。

【0029】この発明の不正アクセス防止方法およびシステムにおいては、複数の支線ネットワークが結合装置により結合されたネットワーク内に1以上の論理グループが構成されている通信ネットワークの該論理グループにおける不正アクセスを防止するために、送信時の通信パケットに含まれるネットワーク内継続時間情報の初期値を、予め通信ネットワーク内に設定した論理グループ内における機密情報として、所定値に定め、前記結合装置が、前記通信パケットの通過時に前記ネットワーク内継続時間情報の妥当性をチェックすることにより、前記論理グループの内外間での通過パケットのフィルタリン

グを行う。したがって、パケットの既存エリアであるネットワーク内存続時間情報を利用して不正パケットのフィルタリングを行うことができ、パケットのデータ形式にエリアの追加を行うことなく、不正パケットの効果的な排除が可能となる。

【0030】

【発明の実施の形態】以下、この発明の実施の形態を図面を参照して説明する。

【0031】この発明の実施の形態に係る不正アクセス防止システムは、TCP/IPプロトコルを用いた通信ネットワークシステムに適用している。この実施の形態では、TCP/IPプロトコルのIPヘッダ内の既存のエリアであるTTLを利用することにより不正パケットのフィルタリングを行うことにより、通信パケットの在来データのままで不正アクセスを効果的に防止する。

【0032】TCP/IPプロトコルによる通信パケットのIPヘッダには、TTL(Time to Live: ネットワーク内存続時間)情報を格納するためのTTLエリアが設けられている。TTL情報とは、通信パケットが、あとどれだけの時間ネットワーク内に存続できるか、すなわち存続残時間を秒単位で示したものである。この存続残時間は、秒単位を基本としているが、処理時間が1秒に満たない場合および処理時間が計測できない場合があり、一般に、例えばルータまたはゲートウェイのような結合装置を通過する度に、その都度“1”マイナスされ、このTTLの値が“0”である通信パケットを検出したときに、その通信パケットは、存続時間が満了したものととして廃棄される。このようなTTL情報は、永遠に配達されずに、ネットワーク中を浮遊するパケットが発生することを防止するために設けられている。TCP/IPプロトコルにおいては、TTLの最大値は“255(秒)”である。一般には、送信端末から受信端末までのルータおよびゲートウェイ等の結合装置の数は、不正パケットの発生を防止するために多めに見積もられる。しかも、このTTLの値は、仮に最大値を設定しても送信から255秒たった時点で通信パケットが廃棄されるため、通常の場合、かなり大きめに設定される。

【0033】この発明では、論理的なグループ内で、TTLの初期値を機密情報として予め取り決めておき、グループ内の送信端末から受信端末までにパケットが通過すると予想されるルータおよびゲートウェイ等の結合装置の最大数を設定しておく。この結合装置の最大数よりも、TTLの初期値を大きく設定しておく。パケットのフィルタリングにあたっては、パケット通過時のTTLの値がTTLの初期値から(初期値-最大通過結合装置数)までの範囲であれば正常パケット、該範囲外であれば不正パケットと判断する。

【0034】このような仕組みにより、グループ内の端末のIPアドレスを使用して不正にグループ内の端末に

アクセスしようとするグループ外の不正な端末からの不正パケットを排除することができる。

【0035】図1～図3を参照して、上述した原理に基づくこの発明による不正アクセス防止システムを組み込んだネットワークシステムの実施の形態を説明する。

【0036】図1は、この発明の実施の形態に係る不正アクセス防止システムを組み込んだゲートウェイの主要部の構成を示している。

【0037】図1に示すゲートウェイ1は、IPヘッダチェック部11およびパケット廃棄処理部12を具備している。

【0038】IPヘッダチェック部11は、IPヘッダの情報をチェックし、IPヘッダに含まれるTTL(Time to Live: ネットワーク内存続時間)情報およびIPアドレス情報に基づいて、当該論理グループの内部から外部へ、および外部から内部への通過パケットをチェックして、不正でない通信パケットのみを通過させ、不正パケットの通過を阻止する。パケット廃棄処理部12は、IPヘッダチェック部11により、通過が阻止された不正パケットを廃棄処理する。

【0039】IPヘッダチェック部11は、TTLフィルタリング部21およびIPアドレスフィルタリング部22を有する。

【0040】TTLフィルタリング部21は、妥当性チェック部21aおよびフィルタリング処理部21bを有し、IPヘッダ中のTTL情報の妥当性をチェックして、TTL情報として妥当性のあるTTL情報を有する通信パケットのみを通過させ、妥当性のないTTL情報を有する通信パケットの通過を阻止する。

【0041】妥当性チェック部21aは、通信パケットの通過時にIPヘッダにおけるTTL情報が所定の条件を満足しているか否かに基づいて、TTL情報の妥当性をチェックする。フィルタリング処理部21bは、論理グループの内外間での通過パケットに対し、妥当性チェック部21aのチェック結果に基づいて、TTL情報が所定の条件を満足している通信パケットのみを通過させ、該所定の条件を満足していない通信パケットをパケット廃棄処理部12に与える。

【0042】上述したようにゲートウェイ1におけるTTL情報を用いたフィルタリングでは、各論理グループにおいて、予めグループ内でのTTLの初期値を機密データとして取り決め、且つグループ内の送信端末から受信端末までにパケットが通過する結合装置、例えばゲートウェイおよびルータ等、の最大数を設定しておく。そして、これらTTLの初期値と最大通過結合装置数をゲートウェイ1の妥当性チェック部21aに予め登録しておくことにより、妥当性チェック部21aは、パケット通過時のTTLの値がTTLの初期値から(初期値-最大通過ゲートウェイ数)までの範囲内であるか否かを条件として妥当性をチェックする。TTLの値が該範囲内

であれば正常パケットすなわち妥当性ありと判定し、当該範囲外であれば不正パケットすなわち妥当性なしと判定する。

【0043】IPアドレスフィルタリング部22は、IPヘッダにおけるIPアドレス情報に基づいて、当該論理グループの外部から当該論理グループの内部のアドレスへの通信パケットおよび当該論理グループの内部から当該論理グループの外部のアドレスへの通信パケットを通過させ、それ以外のIPアドレス情報を有する通信パケットの通過を阻止してパケット廃棄処理部12に与える。

【0044】図1に示したゲートウェイ1を用いて構成したネットワークシステムを図2に示す。図2においては、在来のフィルタリング機能を有するゲートウェイと図1のこの発明によるフィルタリング機能を有するゲートウェイとを用いて不正アクセス防止システムを構成している。

【0045】図2に示すネットワークシステムは、第1のゲートウェイ1、第2のゲートウェイ2、第1の端末3、第2の端末4、第3の端末5、第1の支線LAN6、第2の支線LAN7および第3の支線LAN8を備えている。第1の端末3および第2の端末4は、第1の支線LAN6に結合されており、第3の端末5は第3の支線LAN8に結合されている。第1の支線LAN6と第2の支線LAN7とは第2のゲートウェイ2により結合されており、第2の支線LAN7と第3の支線LAN8とは第2のゲートウェイ1により結合されている。

【0046】第1および第2のゲートウェイ1および2は、それぞれ第2の支線LAN7と第3の支線LAN8との間、および第1の支線LAN6と第2の支線LAN7との間で通信パケット等のデータを転送する。

【0047】第1のゲートウェイ1は、図1に示したこの発明に基づく通信パケットのフィルタリング機能を有するゲートウェイである。すなわち、第1のゲートウェイ1は、この発明によるTTL情報を用いた通信パケットのフィルタリング機能と、在来のIPアドレスを用いた通信パケットのフィルタリング機能とを有している。

【0048】第2のゲートウェイは、在来のゲートウェイであり、IPアドレスを用いた通信パケットのフィルタリング機能のみを有している。

【0049】第2の端末4および第3の端末5が同一グループを構成し、第1の端末3はグループ外の端末であるとする。

【0050】この場合、例えば、端末4と端末5とで構成されるグループ内では、機密データとしてTTLの初期値を“5”と設定しているものとする。また、最大通過結合装置数、すなわち最大通過ゲートウェイ数は、ゲートウェイ1および2が存在するため“2”である。これらの値は、ゲートウェイ1の妥当性チェック部21aに予め設定される。

【0051】グループ外の端末3は、端末4と端末5と

のグループ間で取り決めたTTLの初期値がわからないため、端末3では、TTLの初期値を“32”と設定したものとす。端末4が端末5に通信パケットを送信したときの動作、および端末4が支線LAN6に接続していない状態で端末3が端末4を装って、端末4のIPアドレスに設定して、端末5に不正にアクセスしようとした場合の動作について、図3に示すフローチャートを参照して説明する。図3に示すフローチャートは、図1のゲートウェイ1のIPヘッダチェック部11におけるIPヘッダのチェック処理の流れを示している。

【0052】ゲートウェイ2にはIPアドレスのフィルタリングのみを行うために端末4と端末5のIPアドレスを登録する。ゲートウェイ1には、IPアドレスのフィルタリングのために端末4と端末5のIPアドレスを登録し、且つTTLによるフィルタリングのために、端末4と端末5との間で取り決めたTTLの初期値 α “5”と最大通過ゲートウェイ数“2”とを内部の妥当性チェック部21aに記憶させる。

【0053】まず、端末4が同一グループ内の端末5に通信パケットを送信する場合の動作について説明する。

【0054】端末4は、自分のIPアドレス、つまり発信元IPアドレス、に端末4のIPアドレスを設定し、相手のIPアドレス、つまり宛先(送信先)IPアドレスに相手先端末5のIPアドレスを設定するとともに、TTLには当該グループ間で取り決めた初期値 α “5”をセットして、通信パケットを支線LAN6に送信する。

【0055】送信されたパケットは、ゲートウェイ2で受信される。ゲートウェイ2は、IPヘッダをチェックする。ゲートウェイ2は、発信元IPアドレスが登録されている端末4のアドレスであり、宛先IPアドレスが登録されている端末5のアドレスであるため、正常パケットとみなす。正常パケットとみなすと、ゲートウェイ2は、元のTTL値である“5”から“1”をマイナスした“4”を新たなTTL値としてTTLにセットして、通信パケットを支線LAN7に送信する。

【0056】支線LAN7に送信されたパケットは、さらにゲートウェイ1で受信される。ゲートウェイ1は、IPヘッダチェック部11において、図3に示すフローチャートに従ってIPヘッダのチェックを行う。

【0057】IPヘッダのチェックが開始されると、IPのバージョンのチェックを行い(ステップS11)、バージョンが異常である場合は、パケット廃棄処理部12でパケットを廃棄する(ステップS17)。ステップS11で、バージョンが正常であった場合は、IPヘッダのその他の情報のチェックを行い(ステップS12)、該その他の情報の異常を検知した場合にもステップS17に移行してパケットを廃棄する。

【0058】ステップS12で正常であった場合には、TTLの値が“0”であるか否かのチェックを行う(ス

テップS13)。ステップS13において、TTLの値が“0”である場合には、TTLすなわちネットワーク内存続時間が満了しているので、ステップS17でパケットを廃棄する。この場合には、TTLの値は、“4”であるので、ステップS13では正常と判定され、TTLフィルタリング部21の妥当性チェック部21aでTTLの値の妥当性のチェックを行う(ステップS14)。

【0059】妥当性のチェックは、TTLの値が初期値 α 以下で且つ(初期値-最大ゲート数) β を超えているか否かにより行う。TTLの値がこの範囲内であれば妥当であるとみなす。

【0060】この場合、初期値 α は“5”、(初期値-最大ゲート数) β は“3”(=5-2)であり、受信したパケットのTTLの値は“4”であるため、正常とみなされる。ステップS14で正常とみなされると、IPアドレスフィルタリング部12によりIPアドレスのチェックを行う(ステップS15)。ステップS14で不正とみなされた場合には、ステップS17でパケットを廃棄する。

【0061】受信した通信パケットの発信元IPアドレスは登録されている端末4のIPアドレスであり、宛先IPアドレスは登録されている端末5のアドレスであるため、正常パケットとみなし、通信パケットは、ゲートウェイ1に受信される(ステップS16)。ゲートウェイ1は、受信したパケットのTTLに“4”から“1”をマイナスした“3”をセットして、通信パケットを支線LAN8に送信する。送信された通信パケットは相手先端末である端末5で受信される。

【0062】次に、端末4が支線LAN6に接続されていない状態で、当該グループ外の端末3が端末4を装って不正に端末5にパケットを送信しようとした場合の動作を説明する。

【0063】端末3は、発信元IPアドレスに端末4のIPアドレスを設定し、宛先IPアドレスに相手先端末5のIPアドレスを設定して、通信パケットを支線LAN6に送信する。しかしこの場合、端末3では、相手先端末5が属する論理グループに属していないので、当該グループ内で取り決めたTTLの初期値がわからない。そのため、端末3は、適当な値として“32”をTTLにセットして通信パケットを送信する。

【0064】送信された通信パケットはゲートウェイ2に受信される。ゲートウェイ2は、IPアドレスのフィルタリングのためのIPヘッダのチェックを行うが、発信元IPアドレスが登録されている端末4のアドレスであり、宛先IPアドレスが登録されている端末5のアドレスであるため、IPアドレスは正常であるとみなす。そこで、ゲートウェイ2は、“32”から“1”をマイナスした“31”をTTLにセットして、該通信パケットを支線LAN7に送信する。

【0065】支線LAN7に送信されたパケットはゲートウェイ1で受信される。ゲートウェイ1は、IPヘッダチェック部11において、図3に示すフローチャートに従ってIPヘッダのチェックを行う。

【0066】IPヘッダのチェックが開始されると、ステップS11でIPのバージョンのチェックを行い、バージョンが異常である場合は、ステップS17に移行しパケット廃棄処理部12でパケットを廃棄する。ステップS11で、バージョンが正常であった場合は、ステップS12で、IPヘッダのその他の情報のチェックを行い、異常を検知した場合には、ステップS17でパケットを廃棄する。

【0067】ステップS12で、IPヘッダのその他の情報が正常であった場合には、ステップS13で、TTLの値が“0”であるか否かのチェックを行う。ステップS13のチェックにおいて、もしもTTLの値が“0”であればパケットを廃棄するが、この場合は、TTLの値が“31”であるため、ステップS13では正常と判定され、ステップS14でTTLの値の妥当性のチェックを行う。

【0068】ステップS14の妥当性のチェックにおいて、先に述べたように初期値 α は“5”であり、(初期値-最大通過ゲートウェイ数)である β は“3”(=5-2)であるが、受信した通信パケットのTTLの値は“31”であるため、異常とみなされ、ステップS17に移行して、該通信パケットは廃棄される。

【0069】上述したように、IPヘッダ部分におけるTTLを利用したフィルタリング機能により、IPアドレスフィルタリングでは検出することができない不正パケットを検出し、廃棄して、端末の不正アクセス防止機能の信頼性を向上することができる。

【0070】なお、図1～図3で説明したこの発明の実施の形態においては、TTL情報を利用したフィルタリングに、IPアドレスによるフィルタリングを併用するものとしたが、さらにMACアドレスに基づくフィルタリング処理を行う手段を設けて、MACアドレスフィルタリング機能を併用するようにしてもよい。

【0071】

【発明の効果】以上説明したように、この発明の不正アクセス防止方法およびシステムにおいては、複数の支線ネットワークが結合装置により結合されたネットワーク内に1以上の論理グループが構成されている通信ネットワークの該論理グループにおける不正アクセスを防止するために、送信時の通信パケットに含まれるネットワーク内存続時間情報の初期値を、予め通信ネットワーク内に設定した論理グループ内における機密情報として、所定値に定め、前記結合装置が、前記通信パケットの通過時に前記ネットワーク内存続時間情報の妥当性をチェックすることにより、前記論理グループの内外間での通過パケットのフィルタリングを行う。したがって、パケッ

トの既存エリアであるネットワーク内接続時間情報を利用して不正パケットのフィルタリングを行うことができる。

【0072】すなわち、この発明によれば、パケットの既存エリアを利用した不正パケットのフィルタリングを可能とし、パケットのデータ形式にエリアの追加を行うことなく、不正パケットの効果的な排除を可能とする不正アクセス防止方法およびシステムを提供することができる。

【図面の簡単な説明】

【図1】この発明の実施の形態に係る不正アクセス防止システムを組み込んだゲートウェイの主要部の構成を示すブロック図である。

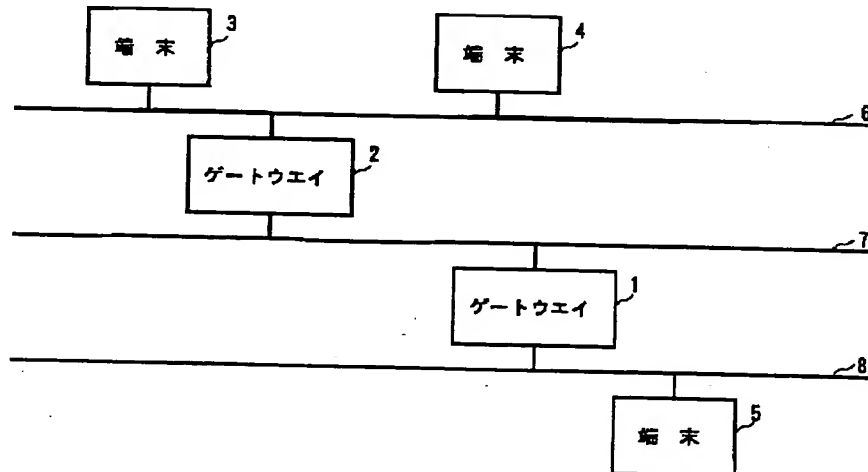
【図2】図1のゲートウェイを用いたネットワークシステムの構成を示すブロック図である。

【図3】図1のシステムの動作を説明するため、ゲートウェイのIPヘッダチェック部におけるIPヘッダのチェックの流れを示すフローチャートである。

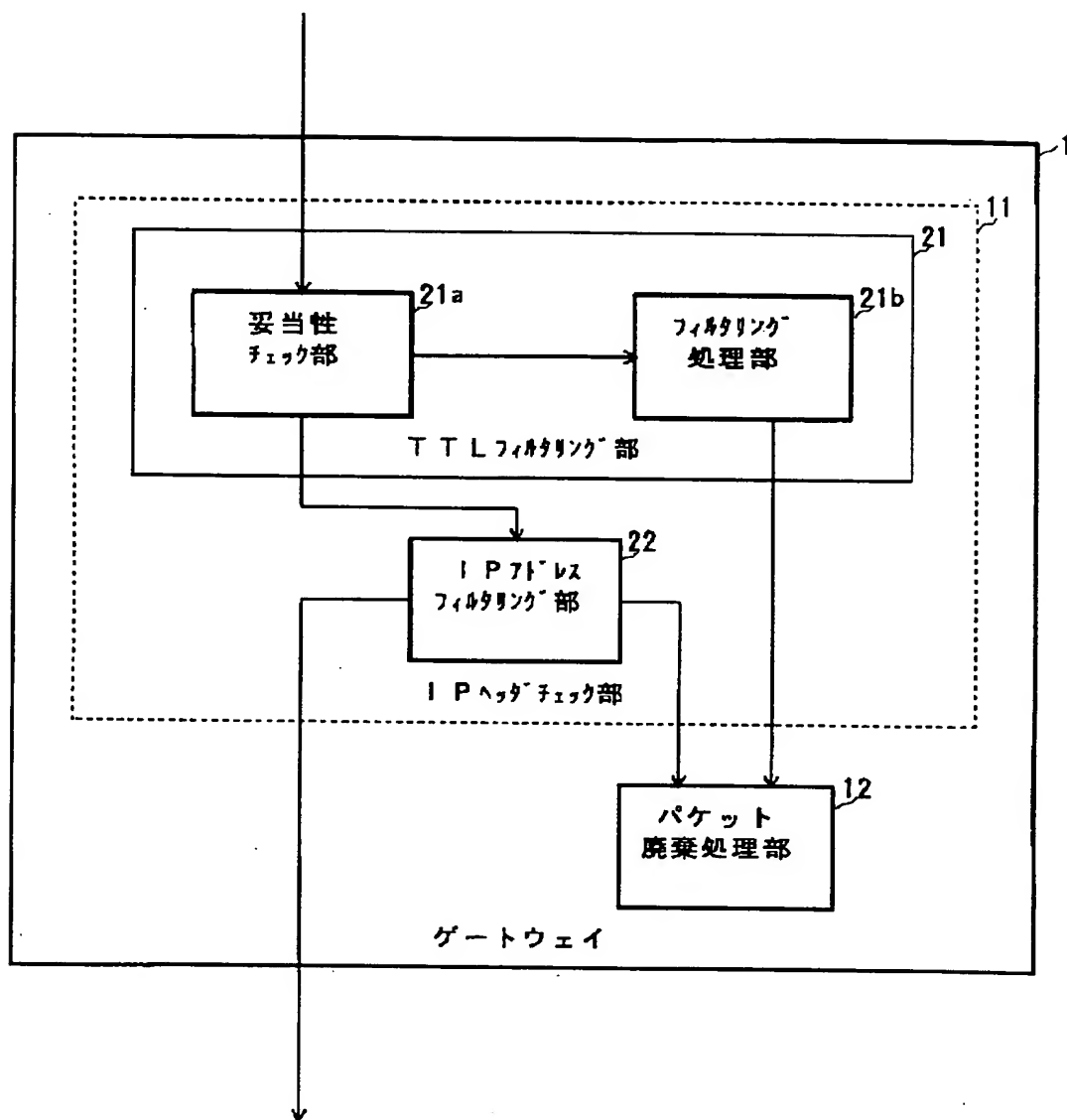
【符号の説明】

- | | |
|------|-------------------------------|
| 1, 2 | ゲートウェイ |
| 3~5 | 端末（端末装置） |
| 6~8 | 支線LAN（Local Area Network） |
| 11 | IP（Internet Protocol）ヘッダチェック部 |
| 10 | 12 パケット廃棄処理部 |
| | 21 TTL（Time to Live）フィルタリング部 |
| | 21a 妥当性チェック部 |
| | 21b フィルタリング処理部 |
| | 22 IPアドレスフィルタリング部 |

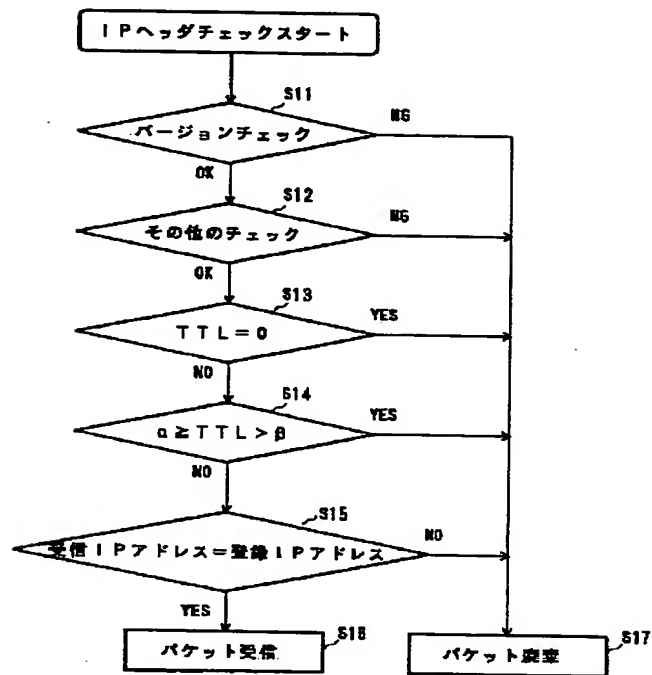
【図2】



【図1】



【図3】



α : TTL初期値
β : TTL初期値 - 最大通過ゲート数